StoreFront Planning Guide

CITRIX®

Contents

Overview

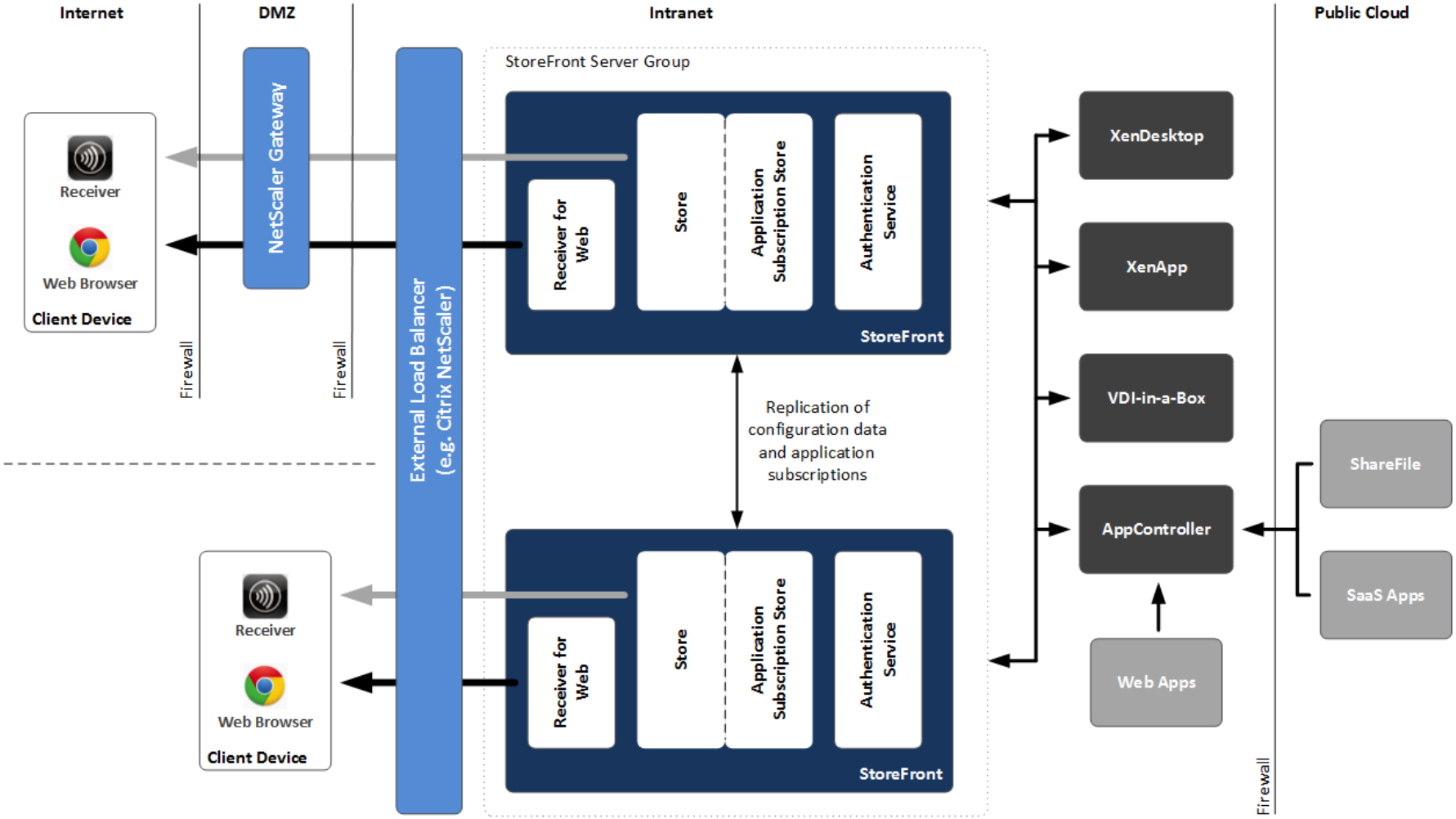
Citrix StoreFront, which is the successor to Citrix Web Interface, authenticates users to XenDesktop sites, XenApp farms, App Controller (SaaS Apps), and VDI-in-a-Box enumerating and aggregating available desktops and applications into stores that users access through Citrix Receiver for Android, iOS, Linux, Windows, Win8/RT or Receiver for Web sites. StoreFront is an integral component of XenDesktop 7 but can be used with XenApp and XenDesktop 5.5 and up deployments. It has been built on a modern, more flexible and powerful framework than Web Interface that enables StoreFront to provide next generation features, such as:

- Unified StoreFront for XenApp and XenDesktop resources that can also deliver SaaS & Native Mobile applications (through App Controller).
- Simplified Account Provisioning, which enables users to connect to assigned desktops and applications by simply entering their email or server address, or by opening a Provisioning File in Receiver.
- Access from any Receiver with a consistent user experience, including automatic fallback to Receiver for HTML5 on Receiver for Web sites if a native client isn't available locally and can't be installed.
- Synchronization of resource subscriptions across all platforms and devices (Follow-me Apps & Data).
- Cross-farm aggregation and de-duplication, that aggregates and delivers a unique set of applications from multiple farms across different sites.
- Farm-Based Optimal HDX Connection Routing, which enables the use of the nearest NetScaler Gateway for HDX traffic routing independent of the NetScaler Gateway used for initial authentication.

This planning guide provides details about the StoreFront architecture and key design decisions for typical deployments.

StoreFront Functionality & Architecture

The following diagram depicts a typical StoreFront infrastructure for environments without XenMobile:



Please refer to CTX138635 - [Citrix Reference Architecture for XenMobile 8.5] for further information about XenMobile deployments.

StoreFront consists of the following components:

- **Authentication service:** This service, which is an integral part of StoreFront, authenticates users to XenDesktop sites, XenApp farms, and App Controller (for SaaS apps). The authentication service ensures that users only need to log on to StoreFront/Receiver once.

- **Store:** The store retrieves user credentials from the authentication service to authenticate users to the components providing the resources. The store also enumerates and aggregates the resources currently available from XenDesktop sites, XenApp farms, and App Controller (SaaS Apps). Users access the store through Citrix Receiver or a Receiver for Web site.

- **Application Subscription Store (Data Store):** This store saves and indexes the application or desktop subscriptions of the users on a per-StoreFront Store basis. In contrast to older versions of StoreFront, where an external Microsoft SQL database was required, the new Application Subscription Store uses the built-in Microsoft Windows Extensible Storage Engine to store details of users' app subscriptions locally on StoreFront servers. When joining a StoreFront server to a Server Group the replication of data between all members is configured automatically.

- **Receiver for Web site:** This site enables users to access stores through a webpage. Furthermore, this site can verify the version of Receiver installed locally on the endpoint and guide the user through an upgrade or installation procedure if required. In scenarios where Receiver cannot be locally Receiver for HTML5 can be enabled for the Receiver for Web sites so that users can access resources directly within HTML5-compatible web browsers.

- **Desktop Appliance site:** Desktop Appliance sites provide users of non-domain desktops with an experience similar to that of users with domain-joined desktops. The web browsers on desktop appliances are configured to start in full-screen mode displaying the logon screen for a Desktop Appliance site. When a user logs on to a site, by default, the first desktop (in alphabetical order) available to the user in the store for which the site is configured starts automatically. Desktop Appliance sites are only created by default when StoreFront is installed and configured as part of a XenDesktop installation.

- **XenApp Services site:** Users with older Citrix clients that cannot be upgraded can access stores by configuring their clients with the XenApp Services URL for a store. This site can also be used from domain-joined desktop appliances and repurposed PCs running the Citrix Desktop Lock.

- **NetScaler Gateway:** Citrix NetScaler Gateway is a physical or virtual appliance, which provides secure remote access to internal resources. The appliance is typically located within the DMZ and exposed to the Internet. When a user connects to NetScaler Gateway they will need to authenticate before any access to internal resources is granted. The access can be controlled by the admin by means of granular application-level policies and action controls.

Users connect to StoreFront using three different methods:

- **Receiver for Web:** This component allows users to access their stores from a web browser. Desktops and applications are launched using the locally installed Receiver or Receiver for HTML5 for clientless access.
- **Native Receiver:** To take full advantage of the features StoreFront has to offer, users should connect into the Citrix environment using Citrix Receiver on their desktop or mobile device. Citrix Receiver is available for Android, iOS, Mac, Window 8/RT, Windows Phone, and soon Linux.
- **XenApp Services Site (PNAgent):** By default, StoreFront creates a XenApp Services site to provide access from legacy devices to the XenApp and XenDesktop resources available in a store. Even though XenApp and XenDesktop resources can be accessed through the PNAgent site, resources from App Controller are not visible. This site enables access from a variety of thin clients, Receiver for Enterprise for specific use cases such as as a seamless desktop experience, Fast Connect, and Desktop Lock for repurposed PCs.

User Logon Workflow

The user logon workflow in StoreFront is different to Web Interface, as detailed in the following table:

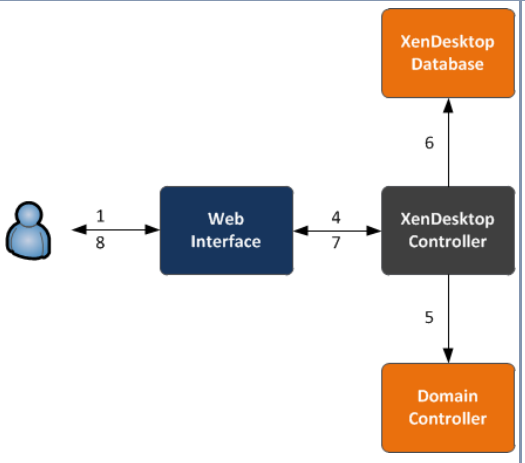
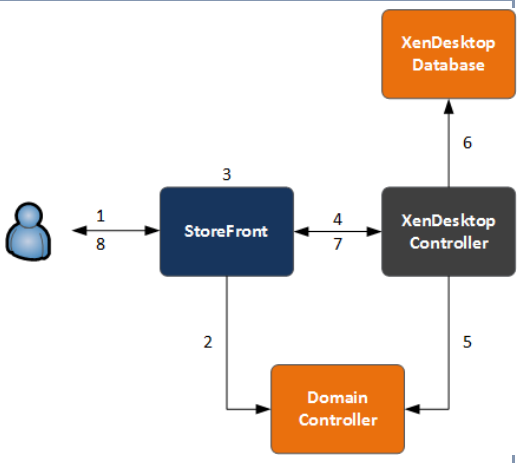
Step	Web Interface	StoreFront
		
1	User enters username and password. This is sent to the Web Interface server.	User enters username and password. This is sent to the StoreFront server.
2		The authentication service of StoreFront fetches the user credentials and validates them with a domain controller. StoreFront servers must reside either within the Active Directory domain containing the user accounts or within a domain that has a trust relationship with the user accounts domain. All the StoreFront servers in a group must reside within the same domain.
3		StoreFront checks the data store for existing user subscriptions and stores them in memory.
4	Web Interface forwards the user credentials as part of a XML query to XenApp or XenDesktop sequentially. In this case, the credentials are sent to the XenDesktop Controller which is the sole resource configured.	StoreFront forwards the user credentials as part of a XML query to the backend systems, such as XenApp, XenDesktop, App Controller or VDI-in-a-Box sequentially. In this case the credentials are sent to the XenDesktop Controller which is the sole resource configured.
5	The XenDesktop Controller validates the user credentials with a domain controller.	
6	After a successful validation the XenDesktop Controller checks which resources have been published to this user within its database.	
7	The XenDesktop Controller sends an XML response to Web Interface / StoreFront which contains all resources available for the user from the XenDesktop site.	
8	Web Interface displays the available resources.	StoreFront sends the list of available resources including the existing subscriptions to the Citrix Receiver installed locally or displays them in Receiver for Web.
End	Now the user can start a resource.	

Table 1: User Logon Workflows

Guidelines

StoreFront plays a critical role in the user authentication process as well as resource enumeration and aggregation of multiple providers. Therefore, designing a StoreFront infrastructure is a vital aspect of an overall Citrix design project.

Within this section critical design decisions will be discussed and recommendations will be provided.

Web Interface or StoreFront

As outlined earlier Web Interface and StoreFront are two different solutions, whose feature sets overlap in many areas, but also offer a variety of distinct features. Therefore it is very important for organizations to review the capabilities of each product against their requirements. In general, it is strongly recommended to build new solutions based on StoreFront, since new features will not be added to Web Interface and end of life has been announced for Web Interface. Furthermore it is important to understand that Web Interface does not support XenDesktop 7 or later. Details on Web Interface lifecycle milestones are available from the Citrix website – Lifecycle Milestones.

While StoreFront goes beyond Web Interface in many areas, StoreFront 2.0 does not support all features of Web Interface. The following tables outlines the Web Interface features that are not currently available in StoreFront:

Area	Feature
Deployment Options	Web Interface on NetScaler (StoreFront is deployable as an application behind NetScaler but runs on separate servers)
Authentication	Delegated Kerberos Authentication
	Active Directory Federation Services (ADFS) 1.0 integration
	Account self-service (SSPR) (reset/unlock with security questions)
	Smart card authentication via browser (Native Receivers required)
	Domain pass through authentication via browser (Native Receiver for Windows required)
	Support for Novell NDS
	Anonymous authentication
Other	Messaging (user notifications)
	Settings per location (IP Subnet)
	Client proxy settings configuration
	Offline Apps (Users cannot access offline applications or App-V sequences through Receiver for Web sites. Native Receiver is required)
	Compact/Low graphics Mode and embedding

Table 2: Web Interface features currently not supported by StoreFront 2.0

High Availability

If the server hosting StoreFront or the respective web service is unavailable, users will not be able to launch new virtual desktops, published applications or manage their subscriptions. Therefore at least two StoreFront servers should be deployed to prevent this component from becoming a single point of failure. An intelligent load balancing appliance (e.g. Citrix NetScaler), which is capable of verifying the availability of the StoreFront service, should be used to load balance users across multiple StoreFront servers. Other less sophisticated load balancing mechanisms, such as Windows NLB, can perform very basic availability checks only (i.e. server up / down) but cannot determine the status of individual services. This could result in users being forwarded to StoreFront servers that cannot process new requests (e.g. server up but web service down).

Recommendation: At least two StoreFront servers should be deployed for redundancy reasons and Citrix NetScaler or another intelligent load balancing solution should be used for load balancing and fault tolerance. To simplify management of the StoreFront infrastructure, both servers should be member of the same StoreFront Server Goup.

Security – Inbound Traffic

Communications from the web browser or Receiver and StoreFront server include user credentials, resource sets, and session initialization files. This traffic is typically routed over networks outside the datacenter boundaries or on completely untrusted connections (such as the Internet). Therefore Citrix strongly recommends that this traffic is encrypted using SSL.

Note: By default, Citrix Receiver requires SSL to connect to StoreFront. This means email-based account discovery or the manual configuration of a StoreFront store in Receiver will not work unless a valid and trusted SSL certificate has been implemented on the StoreFront server and/or the respective external load balancer. However, workarounds exist for environments in which an SSL certificate cannot be implemented.

Windows

1. Navigate to HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\AuthManager (for 64-bit machines, navigate to HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\AuthManager)
2. Create a new String value called ConnectionSecurityMode.
3. Set the value to Any.
4. Navigate to HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Dazzle (for 64-bit machines, navigate to HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\Dazzle)
5. Modify the String value called AllowAddStore to A.

Please refer to eDocs – Configure and install Receiver for further information.

iOS

1. Add a new Store using the “New Accounts” wizard.
2. Change to manual setup.
3. Enable the “Ignore certificate warnings” setting.

Recommendation: Implement trusted and valid server certificates on all StoreFront servers and external load balancers to enable SSL communication between Receiver and StoreFront.

Security – Backend Traffic

User credentials are sent between StoreFront and the XenApp Controllers, XenDesktop Controllers and the App Controller virtual appliance. For example, in a typical session with a XenDesktop Controller, the StoreFront server passes user credentials to the Citrix XML Service for user authentication and the Citrix XML Service returns resource set information. A TCP/IP connection and the Citrix XML protocol is used to pass the information between the StoreFront server and the XenDesktop site. The XML protocol uses clear text to exchange all data, with the exception of passwords, which are transmitted using obfuscation.

Recommendation: For Citrix environments with high security requirements, encrypt StoreFront to XenApp, XenDesktop and App Controller communications. For further guidance on how to encrypt this traffic, please refer to

- eDocs – Use the SSL Relay (XenApp only).
- CTX130213 - How to Configure SSL on XenDesktop 5 Controller to Secure XML Traffic (XenDesktop only).
- eDocs – Use SSL on XenDesktop 7 Controllers (XenDesktop only).

Please refer to eDocs – Secure your StoreFront environment for further information

Delivery Controllers

To provide users with desktops and applications, StoreFront must be configured with the IP address or DNS name of at least one Controller in each XenDesktop site and/or XenApp farm. For fault tolerance, multiple Controllers should be entered for each site and/or farm specified. StoreFront will automatically failover to the second server in the list in case the first server becomes unavailable (active/passive). For large infrastructures or environments with a high logon load an active distribution of the user load (active/active) is recommended. This can be achieved by means of an industry proven load balancer with built-in XML monitors and session persistency, such as Citrix NetScaler.

Recommendation: At least two Controllers should be specified per XenApp farm / XenDesktop site.

Recommendation: For large environments, active/active load balancing of the delivery controllers is recommended.

Beacons

Citrix Receiver uses beacon points (web sites) to identify whether a user is connected to an internal or external network. Internal users are connected directly to resources while external users are connected via Citrix NetScaler Gateway. Citrix Receiver continuously monitors the status of network connections (e.g. link up / link down or change of the default gateway). When a status change is detected, Citrix Receiver will first check that the internal beacon points can be accessed before moving on to check the accessibility of external beacon points. StoreFront provides Citrix Receiver with the http(s) addresses of the beacon points during the initial connection process and provides updates as necessary.

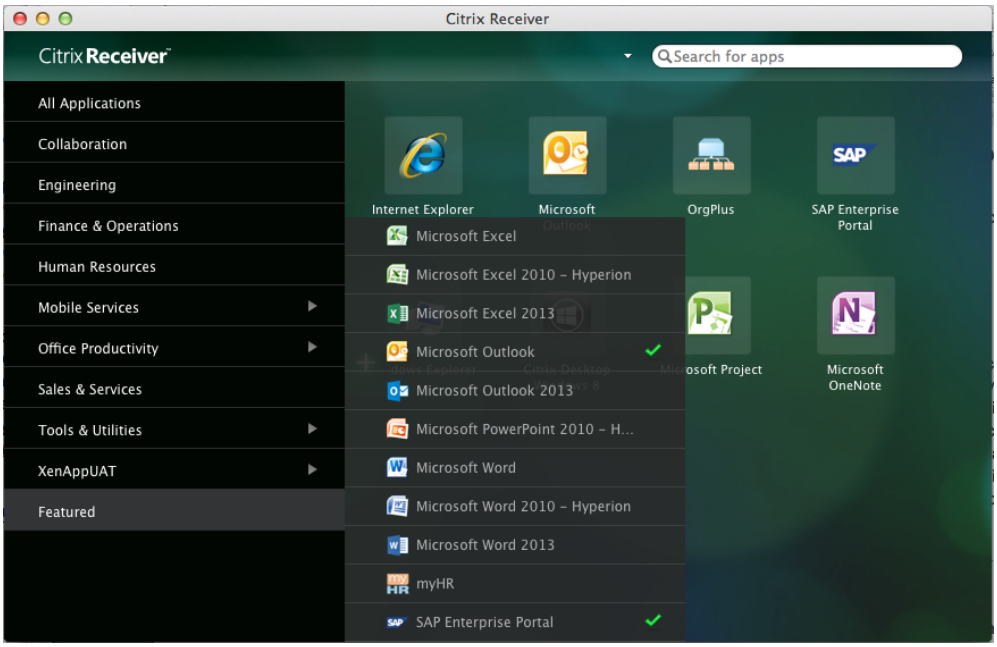
Recommendation: Configure as least two highly available external beacons that can be resolved from public networks so that Citrix Receiver can determine whether users are located behind an Internet paywall, such as in a hotel or Internet café.

It is strongly recommended that highly available websites are specified as beacons.

Auto Provisioned Apps (Keywords)

StoreFront displays applications differently to Web Interface. Instead of having all accessible applications appear on the home screen, first time users are invited to choose (subscribe) to the applications they want to regularly use after they logon. Before a user can launch an application, they must first choose which applications should be placed on their home screen. This approach, deemed “Self-Service” apps, allows users to restrict the applications that they see on their home screen to the ones that they use on a regular basis. The applications chosen by every user for each store are recorded by the subscription store service so that they can be displayed on the Receiver home screen from any device that the user connects from (Follow me Apps).

To avoid users from having a blank screen when they first logon, it is recommended that administrators automatically subscribe users to a few core applications. To do this, add **KEYWORDS:Auto** to the application or desktop description in XenApp or XenDesktop. Another option that can be used to organize applications is **KEYWORDS:Featured**. Unlike the Auto keyword which places certain apps on the home screen, the Featured keyword only places apps in the Featured category (as shown below).



The app will also appear in another category if a Client Application folder has been specified.

In addition the string **KEYWORDS:prefer="application"** can be used to specify that the locally installed version of an application should be used in preference to the equivalent delivered instance if both are available.

For further information please refer to eDocs – Optimize the user experience.

Scalability (preliminary)

The number of Citrix Receiver users supported by a single StoreFront server depends on the hardware specifications and on the level of user activity. At the current point in time, scalability testing for StoreFront 2.0 has not been completed. Early testing results indicate that, a single StoreFront 2.0 server with twin 2 GHz quad-core CPUs and 8 GB RAM supports up to 25,000 user connections per hour in a light usage scenario (users log on, enumerate their resources, and access existing subscribed resources) or up to 6000 user connections per hour in an intensive usage scenario (users log on, enumerate their resources, and then subscribe and unsubscribe to a resource.)

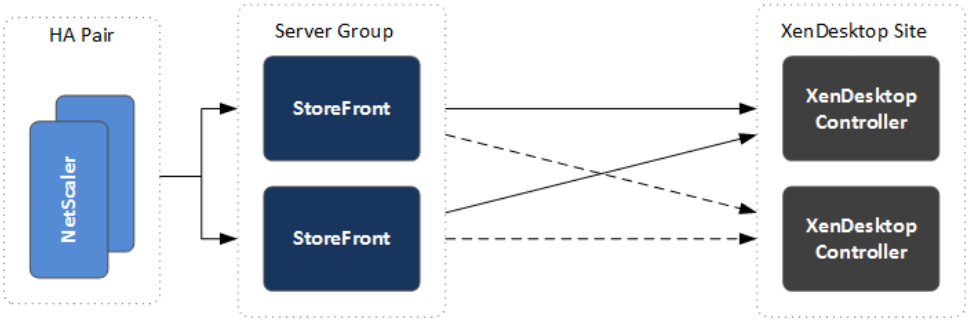
For the optimum user experience, Citrix recommends that not more than 10 XenDesktop, XenApp, App Controller, and VDI-in-a-Box deployments are aggregated in a single store.

Planning

When choosing the optimal StoreFront architecture, it is important to understand the configurations discussed within this document and the requirements of the respective infrastructure. This section outlines three sample customer scenarios, in which we'll follow the topics discussed earlier opting for the simplest and best performing solution.

Scenario 1 – 500 Users

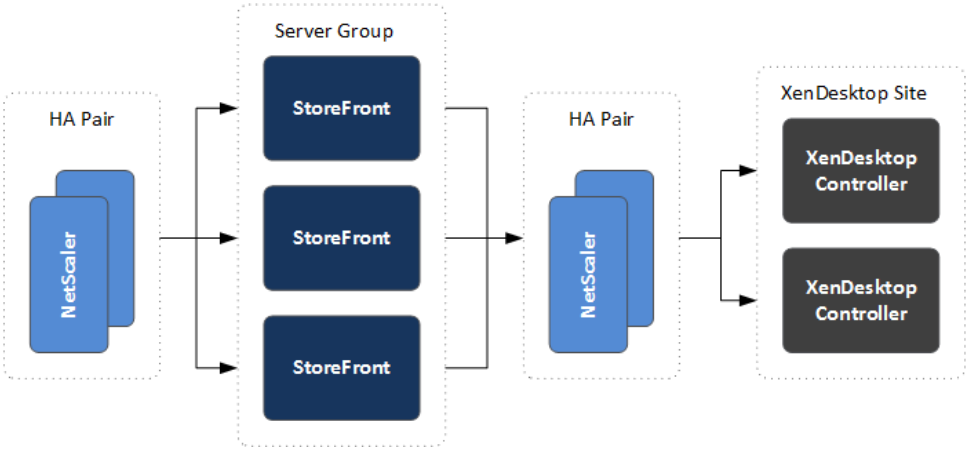
In this scenario 500 users should be supported. The users logon to StoreFront in the morning over a period of 2 hours and connect to their virtual desktop. Users typically they keep their sessions open all-day and occasionally access StoreFront after the initial login.



The load on the StoreFront servers in this scenario can be considered very light. Therefore two StoreFront servers have been chosen for redundancy reasons only. Both StoreFront servers are equipped with 2 CPUs and 2GB of RAM to allow for future growth without requiring changes to the access infrastructure. A pair of NetScaler appliances provide load balancing, SSL offloading and availability monitoring for the StoreFront servers. The XenDesktop Controllers are configured in failover order (active/passive) within StoreFront for simplicity reasons. An active/active load balancing of the XenDesktop Controllers is not required due to the small number of users.

Scenario 2 – 5,000 Users

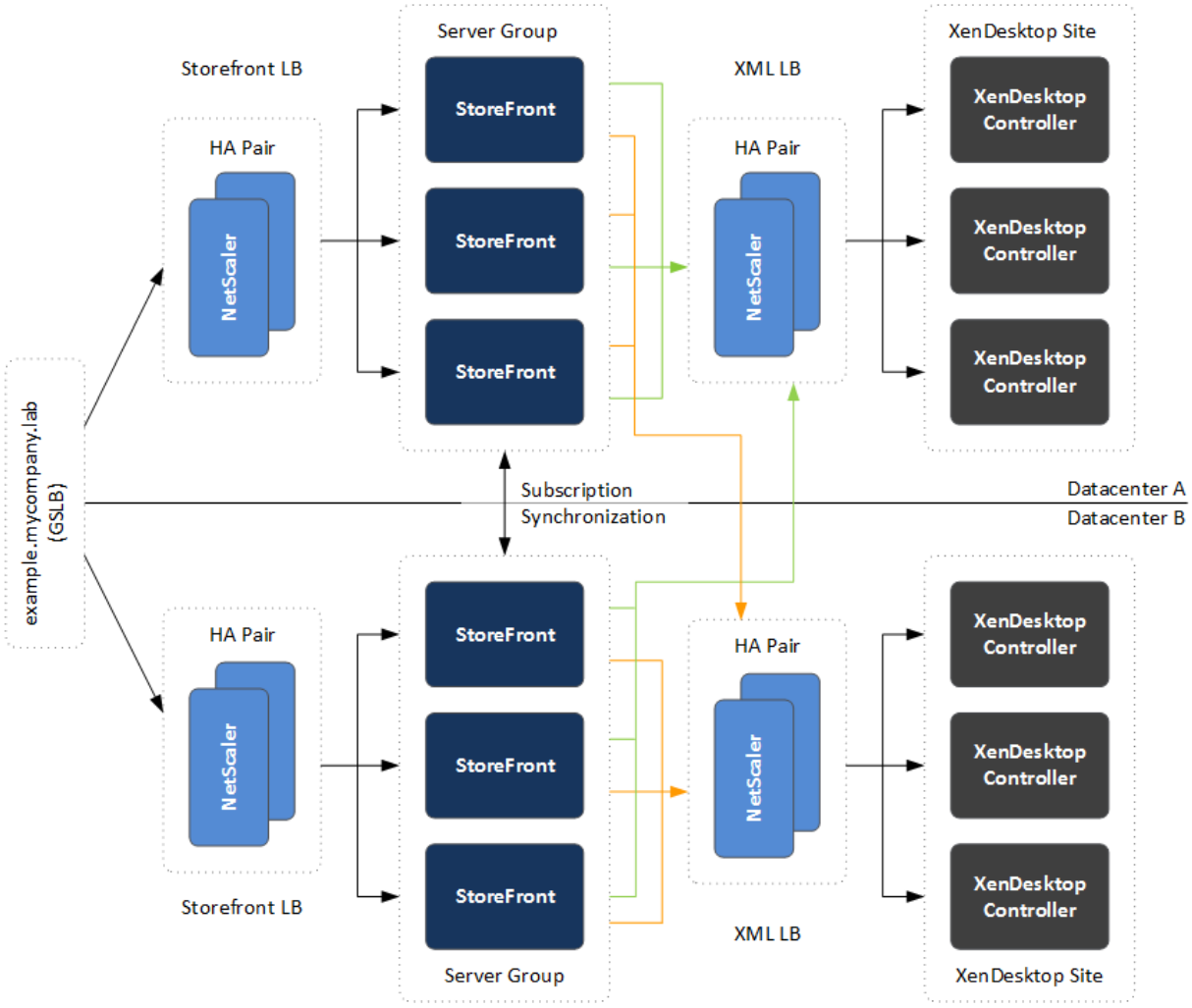
In this scenario, 5,000 users should be supported. As opposed to scenario 1, the users logon to StoreFront in the morning over a very short period of time. Furthermore, users tend to disconnect and reconnect to their desktops multiple times a day.



Due to the high logon load in the morning, three StoreFront servers need to be implemented. All three StoreFront servers are equipped with 2 CPUs and 4GB of RAM to ensure sufficient capacity. A pair of NetScaler appliances provide load balancing, SSL offloading and availability monitoring for the StoreFront servers. Furthermore, these appliances are leveraged to load balance the XML requests sent from the StoreFront servers to the XenDesktop Controllers. This ensures an even distribution of the load among the XenDesktop Controllers and avoids a potential bottleneck. StoreFront is configured to connect to a NetScaler vServer rather than the XenDesktop Controllers directly.

Scenario 3 – 10,000 Users

In this scenario 10,000 users should be supported. Similar to scenario 2, users logon to StoreFront in the morning over a very short period of time and typically disconnect and reconnect to their desktops multiple times a day. As opposed to scenario 1 and 2 the infrastructure needs to be distributed across two datacenters for disaster recovery reasons. The environment should provide 100% tolerance to a full datacenter outage.



To cope with the high logon load in the morning and the constant load during the day three StoreFront servers with 4CPUs and 4GB of RAM are required. Alternatively, two servers with 8CPUs and 8GB of RAM could be implemented. However, to minimize the impact from a single server outage and to have more management and maintenance flexibility a three-server solution is recommended. Because of the 100% tolerance requirement, the same number of StoreFront servers should be implemented in each datacenter.

Users can access the environment by means of the FQDN example.mycompany.lab. The incoming user requests are distributed by means of Global Server Load Balancing (GSLB). This means the NetScaler HA pairs located in both of the datacenters are configured as authoritative DNS servers for the aforementioned FQDN. When a user initiates a connection to the *example.mycompany.lab* FQDN, one of the NetScaler HA pairs (selected randomly) will determine which datacenter is best suited to serve the request. This decision can be based on proximity, home IP subnet or similar

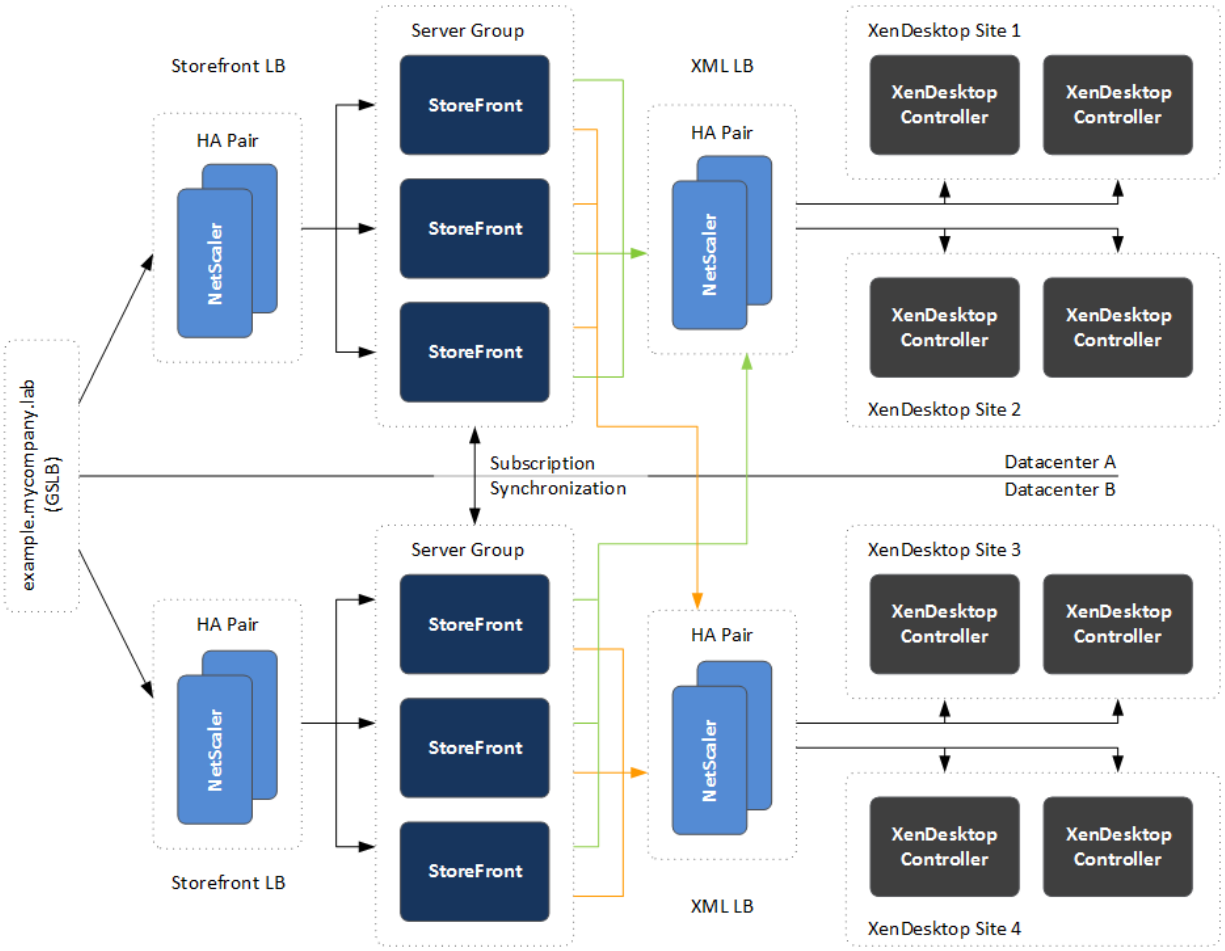
properties of the user. Session persistence is achieved using a client side cookie automatically set by NetScaler.

Since a user can be forwarded to both datacenters, it is required to synchronize the application subscriptions. This can be achieved be means of PowerShell Commandlets as outlined in eDocs - To configure subscription synchronization.

In addition, the NetScaler appliances within each datacenter also provide load balancing, SSL offloading and availability monitoring for the StoreFront servers. These appliances are also leveraged to load balance the XML requests sent from the StoreFront servers to the XenDesktop Controllers. This ensures an even distribution of load amongst the XenDesktop Controllers and avoids a potential bottleneck. StoreFront needs be configured to connect to the NetScaler vServers in both datacenters rather than the XenDesktop Controllers directly.

Scenario 4 – 10,000 Users with Split Sites and Dedicated Home Datacenters

This scenario is equal to scenario 3 except for the fact that the XenDesktop sites have been split into two sites per datacenter to minimize the impact of a XenDesktop site outage. In addition, each datacenter is configured as a home datacenter for 50% of the users. Each user's virtual desktop, user profile, home directory and all user related data is located in their home datacenter. In case of a datacenter outage affected users are redirected to the second datacenter until normal operations can be restored.



In order to meet the aforementioned load balancing and failover requirements, the new StoreFront User Mapping and DR features need to be configured. For this scenario two user groups will be created in Active Directory (Datacenter-A-Users and Datacenter-B-Users). For the Datacenter-A-Users user group, an Aggregation Group consisting of XenDesktop Sites 1 and 2 will be created and configured for load balancing. In addition XenDesktop Site 3 and 4 will be configured for backup only and vice-versa for Datacenter-B-Users. In order to ensure the StoreFront instances in both datacenters behave equally the configuration has to be replicated. When a member of the Datacenter-A-Users user group logs on to StoreFront, the account credentials submitted will be validated and the user is authenticated. StoreFront then determines the user group memberships and verifies if the user already has a session in any of the XenDesktop sites. If that is not the case and the user cannot be reconnected or session sharing cannot be used a new user session is established. In case none of the XenDesktop sites in datacenter A are available, the user will be

redirected to XenDesktop Site 3 or 4. For further information in regards to StoreFront User Mapping and DR, please refer to eDocs - StoreFront high availability and multi-site configuration.

Product Versions

Product	Version
StoreFront	2.0
XenDesktop	7.0

Revision History

Revision	Change Description	Updated By	Date
1.0	Initial Document	Thomas Berger With input from: • Andy Baker – Architect • Saul Romero – Senior Software Eng • Roger LaMarca - Senior Consultant • Matthew Brooks – Architect • Ankur Shah – Prn Product Manager • David Coleman - Director • Daniel Feller – Lead Architect	January 22, 2013
1.1	Update based on feedback	Thomas Berger	February 12, 2013
1.2	Update based on feedback from Richard Eilenberger	Thomas Berger	March 12, 2013
2.0	Updating based on the new features of StoreFront 2.0	Thomas Berger	August 23, 2013

About Citrix

Citrix Systems, Inc. (NASDAQ:CTXS) is a leading provider of virtual computing solutions that help companies deliver IT as an on-demand service. Founded in 1989, Citrix combines virtualization, networking, and cloud computing technologies into a full portfolio of products that enable virtual workstyles for users and virtual datacenters for IT. More than 230,000 organizations worldwide rely on Citrix to help them build simpler and more cost-effective IT environments. Citrix partners with over 10,000 companies in more than 100 countries. Annual revenue in 2011 was $2.20 billion.